OFFICE OF DEPUTY GENERAL COUNSEL
(OPERATIONS)

AGC(IL)-213-08
August 29, 2008

MEMORANDUM FOR THE DEPUTY PROGRAM MANAGER FOR COUNTERTERRORISM SPECIAL PROJECTS, ANALYSIS AND PRODUCTION

SUBJECT: ~~(TS//SI//NF)~~ Assessments of Reasonable Articulable Suspicion Pursuant to Orders of the Foreign Intelligence Surveillance Court – INFORMATION MEMORANDUM

1. (TS//SI//NF) This memorandum reissues OGC guidance to aid in the determinations SID personnel are called upon to make with respect to telephony and electronic metadata under the court orders addressing these subjects with respect to [redacted] Specifically, the memo elaborates on the legal standard applicable to the contact-chaining activities in which SID offices engage pursuant to Business Records Order 08-08 (as well as subsequent Orders for the production of telephony records)[1] as well as to the contact chaining activities in which SID analysts engage pursuant to the Pen Register and Trap and Trace Order 08-110 (as well as subsequent Pen/Trap Orders).[2,3]

---

1 ~~(TS//SI//NF)~~ The Business Records Order is captioned "In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted]

2 ~~(TS//SI//NF)~~ The Pen/Trap Order is captioned [redacted]

3 ~~(TS//SI//NF)~~ OGC memorandum dated October 13, 2006, same subject, is canceled. This memorandum updates the prior memorandum to reflect changes in the Foreign Intelligence Surveillance Court (FISC) authorizations, specifically authorizing access to the data acquired under the Orders for analysis related to [redacted] The substantive guidance concerning the application of the "reasonable articulable suspicion" standard with respect to the authorizations remains unchanged.

2. (TS//SI//NF) Both of the Orders set out a standard that allows access to the data when NSA has identified a known telephone number or other electronic identifier for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that the telephone number or electronic identifier[4] is associated with [redacted][5] provided, however, that a telephone number or an account or address believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. When such a determination has been made, NSA is authorized by the Orders to use such numbers/electronic identifiers as "seed" addresses by querying the accumulated data to determine other telephone numbers or electronic identifiers the seed has contacted.

A. Summary of the Standard

3. (TS//SI//NF) The "reasonable articulable suspicion" standard embodied in the Court's Orders requires that before an analyst may use a telephone number or electronic identifier as a "seed" address to query the database of records, he/she must be able to articulate some fact or set of facts that causes him/her to suspect that the number is associated with [redacted] This formulation means that analysts are not free to use a telephone number or electronic identifier based merely on a hunch or guess, but must instead base their decisions on specific facts that would cause a reasonable person to form such a suspicion.

4. (TS//SI//NF) Note that the standard does not present a particularly high hurdle.[6] The level of evidence demanded by the standard is considerably less than proof by a preponderance of the evidence, meaning that here one need *not* show it is more likely than not that a number is associated with [redacted]

---

[4] (TS//SI//NF) The term electronic identifier is intended to include not only email addresses, but also similar routing and addressing information that effects delivery of electronic communications.

[5] (TS//SI//NF) The phrase "associated terrorist organization" connotes a particular list of terrorist groups designated by the Director of National Intelligence (DNI) to have allied themselves with [redacted] The specific list is included in the FISC orders.

[6] (U//FOUO) The reasonable articulable suspicion standard comes from the law enforcement context and therefore the cases addressing it focus on actions of police officers. *See Terry v. Ohio*, 392 U.S. 1 (1968). The idea underpinning the standard is that the police may stop and briefly detain someone for investigative purposes if the officer involved has a reasonable suspicion supported by articulable facts that criminal activity "may be afoot," even where the officer lacks probable cause to believe that this is so. *See U.S. v. Sokolow*, 490 U.S. 1, 7 (1989). The officer must be able to articulate something more than an "inchoate and unparticularized suspicion or 'hunch.'" *Terry* at 27. Rather, the standard demands some "minimal level of objective justification" for making the stop in question. *INS v. Delgado*, 466 U.S. 210, 217 (1984).

[redacted]. *See Sokolow* at 7. Indeed, the Courts have made clear that the level of suspicion required for a Terry stop – *i.e.* the level of suspicion required to constitute a reasonable articulable suspicion -- is "obviously less demanding than that for probable cause." *Id.* (*citations omitted.*)[7] Further, the *Sokolow* Court observed that the concept of reasonable suspicion, like probable cause, requires an examination of the totality of the circumstances – the whole picture. *Id., citing U.S. v. Cortez,* 449 U.S. 411, 417 (1981). The *Sokolow* Court, quoting one of its earlier cases, noted that "[t]he process does not deal with hard certainties, but with probabilities. Long before the law of probabilities was articulated as such, practical people formulated certain common-sense conclusions about human behavior; jurors as factfinders are permitted to do the same – and so are law enforcement officers." *See Cortez* at 418.

5. (TS//SI//NF) In addition, for reasons set out below, we understand the t[redacted] "associated" to mean engaged in a common enterprise with [redacted] one of the groups designated by the DNI to have allied itself with [redacted] or with someone acting as an agent thereof. Finally, in a case in which an analyst intends to base his suspicion of a number/electronic identifier used by Party A *solely* on contact with Party B, such contact must be direct contact, and it must be more likely true than not true that Party B is a member or agent of [redacted]

B. <u>Association with</u> [redacted]

6. (TS//SI//NF) As we alluded to above, the meaning of the word "associated" is important to the analysis, since the determination that must be made is that a telephone number or electronic identifier is associated with [redacted] one of the groups designated by the DNI to have allied itself [redacted] While this standard does not say explicitly that the telephone number or electronic identifier at issue must be *used by* a member or agent of [redacted] and while we do not insist on such a finding here, we note that the dictionary definition of "associate" suggests a knowing relationship and engagement in a common enterprise.[9] Therefore, in making their assessments, analysts should consider whether, given the totality of the circumstances, there exist articulable reasons to think that a telephone number or electronic identifier bears a relationship to [redacted] or one of the groups designated by the DNI to have allied itself

---

[7] (U) Reasonable articulable suspicion is a low standard of proof. The common standards of proof and common applications of the standards are set out in Enclosure 1.

[8] (TS//SI//NF) For example, if Party B is a known [redacted] would meet the standard for chaining. Thus, Party B's association with [redacted] requires a probable cause or higher showing.

[9] (U//FOUO) For example, "associate" is defined as follows: "to join as a partner, friend or companion; to keep company with;" and also: "to combine or join with other parts." Merriam Webster Collegiate Dictionary, Tenth Edition, at 70.

[redacted] of a nature that suggests it is used by someone engaged in a common enterprise with one of the aforementioned.

7. (TS//SI//NF) We recognize too that there may be cases in which an analyst's reasonable articulable suspicion that a number is associated with [redacted], will be based on telephone or e-mail contacts alone. While basing a determination on more information than this is preferable (and indeed is required to the degree more information is available, since one is required to examine the totality of the circumstances), analysts must when premising their determinations solely on contact be mindful of what they actually know about the parties involved. For example, an analyst who has reasonable articulable suspicion with respect to a particular telephone number could not query the database to determine what number is three "hops" away in the communications chain, and then, based on such contact alone, conclude that the number three hops away now should be used as a seed number. Therefore, in cases in which communications contacts are the sole justification for concluding that a number is associated with [redacted] such contact must (1) be direct contact, and (2) must be with a number or electronic identifier for which we have concluded it is more likely than not used by a member of [redacted]

C. First Amendment Considerations

8. (TS//SI//NF) In addition, the Orders each contain a provision stating that a telephone number or electronic identifier believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution.

9. (TS//SI//NF) We read the Orders as barring NSA from concluding -- based on such things as the religion of the U.S. person, or his editorials contending that the United States is wrong in its war on terrorism, or his membership in groups that oppose policies of the United States, or the fact that he/she attends anti-war demonstrations and urges his

---

10 (TS//SI//NF) In order to establish a meaningful association from contact alone between the two numbers, A and B, where B is a number that is already suspect, it must be more likely true than not true that number B is used by e.g., a member or agent of [redacted] Neither vague statements about the role of Party B in [redacted] nor an indirect linking of the number in question with Party B (e.g., Party A was in contact with Party X, who was in contact with Party B, who is probably a member of [redacted] will suffice on their own to satisfy the standard as to Party A. Where the reasonable articulable suspicion comes from contact alone, such contact must be direct with a member or agent of [redacted], and it must be more likely than not that our designation of such member or agent is in fact accurate. This advice should help serve to prevent the potential for endless "bootstrapping." As we have discussed, the danger in carrying out the instructions in the Court's Order is a suspicion that ceases to be reasonable because of the tenuousness of the [redacted] connection. We believe that this analytic framework will go a long way to countering any such tendency that might exist. See enclosure 2.

Congressman to cut off funding for U.S. troops in Iraq – that his number or electronic identifier is therefore associated with [redacted] But, as we have already made clear, we do not read the Order to preclude under all circumstances the conclusion that a number is associated with [redacted] solely on the basis of its communications [redacted] and, more specifically, based on its contacts with numbers about which NSA has the appropriate level of suspicion. Our conclusion is supported by First Amendment law, as we discuss below.

10. (U//~~FOUO~~) The First Amendment by its terms makes clear that Congress can make no law respecting the establishment of religion, or abridging freedom of speech or of the press, or peaceable assembly, or the petitioning of the government for the redress of grievances.

11. (U//~~FOUO~~) In addition, the Amendment has also been construed by Courts to protect the freedom of association, a freedom not explicitly mentioned in its text. The Courts have opined that the right of association implied in the Constitution mainly protects associations when they are derivative of other First Amendment guarantees – normally speech, assembly and petition. For instance, in a case examining a university's decision to refuse recognition to a student organization, Students for a Democratic Society, the Supreme Court stated: "While freedom of association is not explicitly set out in the Amendment, it has long been held to be implicit *in the freedoms of speech, assembly and petition*. *Healy v. James*, 408 U.S. 169, 181 (1972) (*citations omitted*) (emphasis added). Similarly, in one of many cases in which the issue was whether the government could compel an organization to turn over lists of its members, the Supreme Court observed that "[i]t is now beyond dispute that freedom of association for the purpose *of advancing ideas and airing grievances* is protected by [the constitution] from invasion by the States." *Bates v. City of Little Rock*, 361 U.S. 516, 522-523 (1960) (*emphasis added*).[11]

12. (U//~~FOUO~~) By contrast, simple social contacts that do not rise to the level of organizations or associations erected for the purpose of engaging in speech do not enjoy the same degree of protection. For example, the Supreme Court, addressing the question whether the state could restrict admission to dance halls to persons between 14 and 18 years old, rejected a challenge based on the right of association and held that the state did indeed have such authority. In so doing, the Court found that there does not exist a "generalized right of 'social association' that includes chance encounters in dance halls." *See City of Dallas v. Stanglin*, 490 U.S. 19, 25 (1989).[12]

---

[11] (U) The First Amendment also protects "intimate associations" among family members, permitting the government to infringe on such interests only to serve a compelling interest, and to do so in the manner that is least intrusive. *See, e.g., Roberts v. United States Jaycees*, 468 U.S. 609, 619-620 (1984).

[12] (~~TS//SI//NF~~) We note also that the very object of the overall effort supported by these Orders is to determine whether or not particular individuals are members of or are associated with the terrorist organizations named in the Orders. Thus, under these Orders, simply by being a member of a named group one becomes subject to government scrutiny.

13. ~~(C)~~ The fact that these Orders only concern communications routing information, or metadata, rather than the substance of communications, further underscores the limited relevance of the First Amendment in the context of association. The D.C. Circuit observed in 1978 that data-gathering activities using legitimate investigative techniques do not violate the First Amendment, at least where no Fourth Amendment privacy is infringed. *See Reporters' Committee for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1064 (D.C. Cir. 1978). Since individuals do not enjoy a reasonable expectation of privacy under the Fourth Amendment in the communications metadata NSA acquires under these Orders, *Smith v. Maryland*, 442 U.S. 735 (1979), the investigative techniques NSA uses pursuant to the Orders do not run afoul of the First Amendment. As the Court in the *Reporters' Committee* case observed, the First Amendment offers no procedural or substantive protection from good faith criminal investigation beyond that afforded by the Fourth and Fifth Amendments. *Reporters' Committee* at 1057.

14. ~~(TS//SI//NF)~~ The above makes clear that the Courts have fashioned protections for association in order to preserve the other rights guaranteed by the Constitution in the First Amendment. Since the right to free association has been found by Courts to be protected largely as an extension of the other constitutional protections in order to keep these rights from being frustrated, and because the derivative right to associate is subsumed by the more specific rights enumerated in the Amendment, we conclude that the terms of the Court's Orders are not intended in the context of these Orders to preclude entirely the conclusion of association based on communications contact observed in communications metadata. We therefore advise that NSA is obligated by the terms of these Orders to refrain from finding an association with [redacted] based solely on these activities that are explicitly afforded protection by the language of First Amendment. But NSA is not precluded from finding an association based on direct contact with a member of [redacted] so long as such contact is direct and the evidence shows it more likely than not that the putative member of an aforementioned group is in fact a member.

D. <u>Summary</u>

15. ~~(TS//SI//NF)~~ Analysts making a determination as to whether a telephone number or electronic identifier is eligible to be a "seed" must consider all the facts that they know or reasonably can know prior to engaging in contact chaining. Looking at the totality of the circumstances, the whole picture, they must determine whether a reasonable articulable suspicion exists that the telephone number or electronic identifier is associated with [redacted] is there reason to suspect that the person using the telephone number is in league with [redacted]. The evidence required is considerably less than a showing that it is more likely than not that a number is associated with one of the aforementioned. Rather, there must be an articulable reason, constituting

more than a hunch, for suspecting that a number is associated with al [redacted]. In cases where a number or identifier is suspicious based solely on its contact with another number or identifier, it must be more likely than not that the other number is used by a member or agent of [redacted] and the contact between the two numbers must be direct contact.

16. (U//~~FOUO~~) We hope this information is useful to you. Enclosure 3 to this memorandum is a chart that sets out the most typical sources of information on which NSA analysts rely in making assessments of reasonable articulable suspicion. If you have questions or would like assistance in making determinations, please contact attorneys in the office of the Associate General Counsel (Intelligence Law) at [redacted]. An attorney is available 24/7 and can be reached after hours through NSOC.

[redacted]

for [redacted]

Deputy General Counsel
(Operations)

Encls:
a/s

cc: Chief of the Homeland Security Analysis Center
Deputy Chief of the Homeland Security Analysis Center
Homeland Mission Coordinators

Enclosure 1

The following chart sets out common standards of proof, the level of proof required in legal actions to discharge the burden of proof, as well as common applications of the standard. The standards are listed from the highest standard to the lowest.

Standard of Proof	Application
Beyond a Reasonable Doubt	Required for criminal conviction.[1]
Clear and Convincing Evidence	Required to prevail in some civil actions.[2]
Preponderance of Evidence	Required to prevail in most civil cases. The standard is met if the proposition is more likely to be true than not true.
Probable Cause	Required for search and arrest warrants.[3]
Reasonable Articulable Suspicion	Required for "Terry" (investigative) stop; see pp. 2-3 of memorandum.

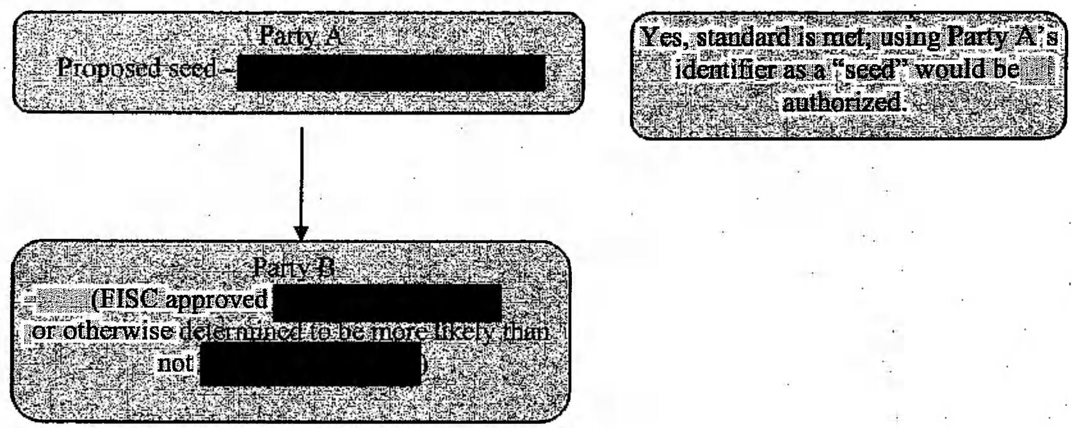
[1] This standard historically has been reserved for criminal cases. The Supreme Court has held that "the Due Process Clause protects the accused against conviction except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime with which he is charged." *In re Winship*, 397 U.S. 358, 364 (1970).

[2] A landmark Supreme Court case reviewing the standard of proof required for involuntary commitment of an individual held that an individual's "interest in the outcome of a civil commitment proceeding is of such weight and gravity that due process requires the state to justify confinement by proof more substantial than a mere preponderance of the evidence." The Court held that the "clear and convincing" standard was required to meet due process guarantees.. *Addington v. Texas*, 441 U.S. 418, 427 (1979).

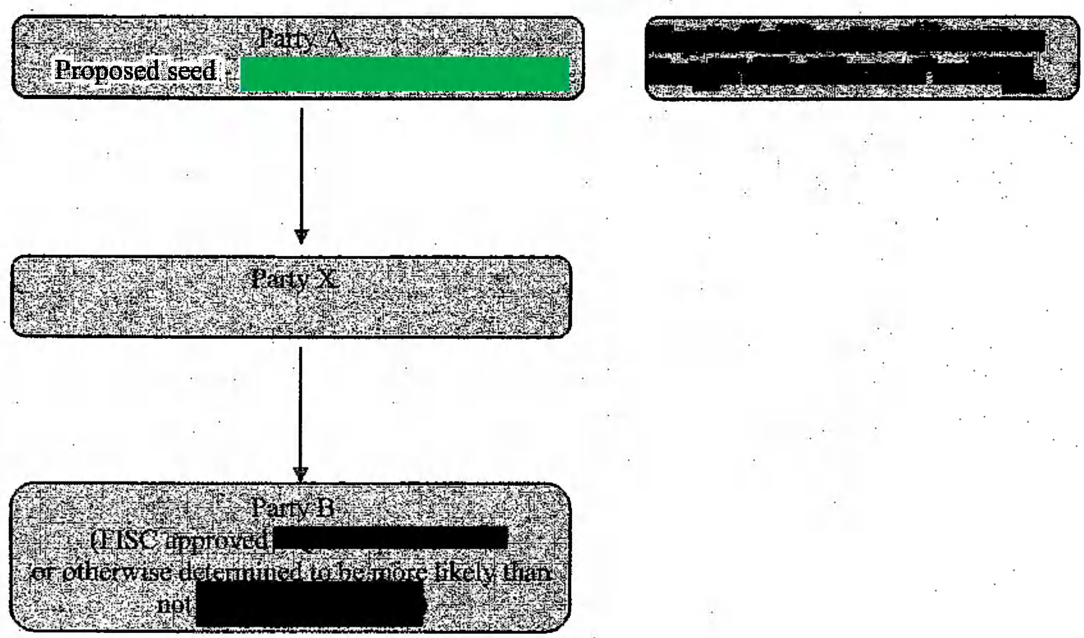
[3] The Supreme Court has held probable cause to mean "a fair probability that contraband or evidence of a crime will be found." *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

Enclosure 2
Use of telephone number or electronic identifier as Seed based on contact alone

- Unknown Party A using [redacted] is in contact with Party B. Absent additional information, in order to use [redacted] as a "seed," the contact with Party B must be direct and it must be more likely than not that Party B is [redacted]



- Unknown Party A using [redacted] is in contact with Party X who is in contact with Party B who is [redacted]. Absent additional information, Party A's [redacted] may not be used as a "seed."



Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: ~~30320726~~

Enclosure 3

The following chart sets out the most typical sources of information on which NSA analysts rely in making assessments of reasonable articulable suspicion. Whatever the source, the analyst proposing to engage in contact chaining or [redacted]eeds to be able to articulate facts that give rise to a reasonable articula[redacted] telephone number or electronic identifier is associated with [redacted]

In addition, analysts must comply with the other procedures set out by the Court authorization or management for effecting the chaining.

FBI	Information satisfying the standard that FBI has in any of the following: • Published report • Preliminary investigation • Full Field investigation • FISA[1]
CIA	Information satisfying the standard that CIA has in any of the following: • Published CIA report • Electronic copy of a sensitive case file cable, which is similar to an FBI preliminary investigation or full field investigation. CIA will provide a reference with date to the cable traffic. • FISA[2]
NCTC	Information satisfying the standard that NCTC has in any of the following: • Published report
NSA	Information satisfying the standard that NSA has in any of the following: • Published NSA report • Unpublished SIGINT collection where research and analysis have led to the discovery of new [redacted] • [redacted]

[1] The standard for chaining on a proposed seed is met when [redacted] selector currently the subject of a FISC authorization pled as [redacted] provided there isn't additional conflicting information; the totality of the circumstances related to a proposed seed must be reviewed.

[2] See footnote 1 above.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

	• [redacted] • Collection/analysis showing [redacted] target using [redacted] • SIGDEV work which is tied to published information or part of a target development effort • Intercepted communication during which an e-mail address or telephone number [redacted] • Known contact with a unique electronic identifier [redacted] already known to be associated with [redacted] where the contact may not have been captured in the meta data chain and may come from other SIGINT sources • Information contained in target knowledge databases, to include the [redacted] and the S2I4 Station table • Information obtained through forensic analysis of seized media belonging to a member of [redacted]
[redacted]	Information satisfying the standard that the [redacted] has in any of the following: • Published [redacted] report • SIGDEV work which is tied to published information
[redacted]	Information satisfying the standard that the [redacted] has in any of the following: • Published report • Transcripts
Public Record	Facts reliably in the public record (e.g., a newspaper article, public internet postings)

FISA Metadata Collection (PRTT)

FISA Collection Verification Requirements:

Verify that the data is [redacted] described in the order.

Verify that the data is of the type authorized by the order (i.e., metadata).

Under no circumstances may the content of communications be collected under this order.

Specific Court-Ordered Procedures and Restrictions:

Storage

Metadata must be stored separately and may not be co-mingled with other metadata.

Data may be kept on-line for 4.5 years (54 months) from the date of acquisition.

Data older than 4.5 years (54 months) from the date of acquisition must be destroyed.

Access

Access to the data is limited to specifically cleared analysts and administrators.

All queries must have prior approval of one of the following:

a) SID Deputy Program Manager for Counterterrorism Special Projects, Analysis and Production
b) Chief Homeland Security Analysis Center
c) Deputy Chief Homeland Security Center
d) Homeland Mission Coordinator.

Automatic log must be generated for each occasion when the info is accessed. Log must contain: a) user login, b) user IP address, c) date and time, d) retrieval request.

Metadata may be accessed only through the use of contact chaining [redacted] described in the FISA application.

Seed accounts must be particular known accounts or addresses that meet the targeting standard articulated by the Court (i.e., based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, that there are facts giving rise to a reasonable articulable suspicion that such account or address is associated with [redacted]

No targeting U.S. persons based upon 1st Amendment protected activities.

OGC must review and approve targeting of U.S. persons to ensure that standards are met.

No queries on the basis of seed addresses that have been validated using [redacted] information. ([redacted]).

Training & Oversight

OGC must train the analysts on the targeting standard and retrieval, storage, and dissemination procedures.

OGC must monitor the designation of individuals with access to such information and the working of the automatic logging/auditing device.

OGC must conduct two random spot checks of [redacted] to ensure that [redacted] are configured and functioning properly.

Minimization Rules

USSID 18 minimization procedures must be applied to the activity.

Chief of Information Sharing must approve dissemination of USP identities as necessary to understand or assess the foreign intelligence.

Duration of the Collection

FISA order is valid for 90 days.

<u>Reporting and Renewal Requirements</u>

File a report to the Court every 30 days containing:

1. a discussion of the queries that have been made since the last report, and a description of how we applied the standard for targeting;
2. any change in the description of the [redacted]

When we seek renewal, a report that includes:

1. detailed information regarding any new facilities proposed to be added;
2. any changes in the proposed means of collection to include [redacted]

FISA Business Records Telephony Metadata Collection

Verification Requirement:

Verify that the data is of the type authorized by the order (i.e., call-detail records/ telephony metadata). (See page 2 of the Order.)

Under no circumstances may the substantive content of communications be received under this order.

Specific Court-Ordered Procedures and Restrictions (see pages 5-12 of the Order):

Standard for Accessing Data

Any search or analysis of the data archive shall occur only after a particular known telephone number has been associated with [redacted] Seed queries must be particular known telephone numbers that meet the targeting standard articulated by the Court --based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted] provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. (See Order, ¶ 3(A).)

No targeting U.S. persons based upon 1st Amendment protected activities.

OGC must review and approve targeting of U.S. persons to ensure that standards are met.

Other Access Requirements

Access to this data is limited to authorized analysts. NSA's OGC shall monitor the designation of individuals with access to the archive. Access to the archive shall be controlled by user name and password. When the metadata archive is

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: ~~Source Marked X1~~

accessed, the user's login, IP address, date and time, and retrieval request shall be automatically logged for auditing capability.

All queries must have <u>prior</u> approval of one of the following:

a) SID Program Manager for Counterterrorism Special Projects
b) Chief, Homeland Security Analysis Center
c) Deputy Chief, Homeland Security Analysis Center
d) Homeland Mission Coordinator

The above individuals must establish management controls for access to the data.

Automatic log must be generated for each occasion when the info is accessed. Log must contain: a) user login, b) user IP address, c) date and time, d) retrieval request.

<u>Manner of Accessing Data</u>

NSA is permitted to perform two sorts of queries: 1) contact chaining to a third tier of contacts, and 2) [redacted]

<u>Storage</u>

Metadata must be stored and processed on a secure private network that NSA exclusively will operate.

Metadata received under this Order may be kept online for 5 years and then destroyed.

<u>Training & Oversight</u>

OGC must train analysts concerning the authorization and querying standard, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of the archived data.

OGC must monitor the designation of individuals with access to the data and the functioning of the automatic logging/auditing.

OGC must conduct two random spot checks during the authorization period to ensure that NSA is receiving only data as authorized by the Court and not receiving the substantive content of communications.

DoJ shall conduct a review at least twice every 90 days of a sample of NSA's queries against the data.

The IG, OGC and SID Oversight must periodically review the program.

Minimization Rules

USSID 18 minimization procedures must be applied to the activity.

Prior to dissemination of any U.S. person identifying information, the Chief of Information Sharing Services must determine that information identifying U.S. persons is related to counterterrorism information and that it is necessary to understand or assess the counterterrorism information.

Duration of Authorization

FISC order is valid for 90 days.

Reporting and Renewal Requirements

NSA must file a report every 45 days with the Court that includes:

1. the queries that have been made since this Order was granted;
2. the manner in which NSA applied the standard required by the Court for accessing the data, and
3. any proposed changes in the way in which the call-detail records would be received.